Module Three

U.S. Policies, Directives, Standards and Guidelines

This module identifies a document that describes the evolution ofinformation security (INFOSEC), communications security (COMSEC), andcomputer security (COMPUSEC). It also describes the U.S. policies, directives, standards and guidelines that exist for trusted system design, development,evaluation, certification, and accreditation. An overview of the purpose andcontents of each policy, directive, standard, and guideline is given along with a list of users that each document applies to.

Module Learning Objectives

The material presented in this module can be read independently of theother modules. Upon completion of this module, the student should:

1. Be familiar with the evolution of INFOSEC, COMSEC, and COMPUSEC.
2. Be aware of each U.S. policy and directive related to trusted system development.
3. Be aware of each U.S. standard and guideline applicable to the design, development, evaluation, certification, and accreditation of trusted systems.

Overview

This module is a reference library. It is intended to provide an annotated bibliography of the many U.S. policies, directives, standards and guidelines related to trusted systems. Some of the documents described are included as required readings of other modules in this course. The descriptions of the documents are intended to help guide the reader through the maze ofpolicies , directives, standards, and guidelines, and make the reader aware of the contents and purpose of each of them. At the end of this module, the reader should at least be aware of what regulations and guidance are available.

Evolution of INFOSEC/COMSEC/COMPUSEC

The evolution of INFOSEC, COMSEC, and COMPUSEC is described in an excellent manner by Chapter 2 of G. T. Gangemi's book *Secure Systems Long Range Strategic Plan* to be published by Wang Laboratories [Gangem90]. This chapter is reprinted here with permission and included as the module's only required reading.

United States Policies and Directives

Copies of U.S. Policies and Directives may be ordered through:

Superintendent of Documents
U. S. Government Printing Office
Washington, D.C. 20402
Phone (202) 783-3238

DOD Directive 5200.28, Security Requirements for Automated InformationSystems (AISs), 11 April 1988 [AIS88]

Purpose: Updates the DoD-wide program for automated information system(AIS) security. Provides mandatory minimum AIS security requirements. Promotes the use of cost-effective, computer-based (e.g., hardware, software, and firmware controls) security features for AISs. Requires a more accurate specification of overall DoD security requirements for AISs that process classified or sensitive unclassified information. Stresses importance of life-cycle management approach to implementing computer security requirements. This is the document that requires “C2 by ‘92.”

Users: Office of the Secretary of Defense, Military Departments and Military Services within the Departments, the Joint Chiefs of Staff (JCS) Unified and Specified Commands, and DoD Components.

DoD 5200.1-R, Information Security Program Regulation, 28 April 1987 [ISPR87]

Purpose: This regulation establishes a system for classification, downgrading and declassification of information; sets forth policies and procedures to safeguard such information; and provides for oversight and administrative sanctions for violations.

Users: Pursuant to the provisions of E.O. 12356 [NSI82], the National Security Council will provide overall policy direction, Heads of DoD Components, senior DoD officials having DoD-wide authority, Director NSA/Chief Central Security Service, Military Departments.

DoD 5220.22-M, Industrial Security Manual for Safeguarding ClassifiedInformation, January 1991 [ISM91]

Purpose: It establishes uniform security practices within industrial plants, educational institutions, and all organizations and facilities used by prime contractors and subcontractors having classified information of the DoD, certain other executive departments and agencies, or certain foreign governments. It establishes requirements for safeguarding all classified information.

Users: Anyone outside of the DoD that is responsible for the security andsafety of government classified material, typically contractors and subcontractors working with the Federal Government.

DoD 5220.22-S-2, Marking Supplement to Industrial Security Manual for Safeguarding Classified Information, September 1987 [ISMM87]

Purpose: This supplement, together with DoD 5220.22-M [ISM91], provides guidance to industry for marking classified information. It provides numerous examples of how to properly mark classified material with the appropriate classification markings.

Users: The authors or the approver of classified information who must ensure the propriety of security classification markings, the administrative personnel who must prepare the finished product, and other personnel who generate or access the classified information.

DoDD 5215.1, DoD Computer Security Evaluation Center, January 1981 [CSEC81]

Purpose: Establishes and defines the roles and responsibilities of the(renamed) National Computer Security Center (NCSC). Specifies their responsibility for the development of specifications, standards and guidelines for trusted systems for the DoD. Tasks the NCSC to champion the widespread availability of commercially developed trusted systems, and to evaluate the trust of those systems.

Users: NCSC and other DoD services and agencies.

NSD-42, National Policy for the Security of National Security Telecommunications and Information Systems, July 1990 [NSTIS90]

Purpose: Provides objectives, policies, and an organizational structure to guide the conduct of national activities directed toward safeguarding systems which process or communicate sensitive information from hostile exploitation; establishes a measure for policy development; and assigns responsibilities for implementation.

Users: Systems Security Steering Group: Secretary of State, Secretary of Treasury, Secretary of Defense, Attorney General, Director of the Office of Management and Budget, Director of Central Intelligence Agency, and the Assistant to the President for National Security Affairs.

The National Telecommunications and Information Systems Security Committee, Secretary of Commerce, Secretary of Transportation, Secretary of Energy, Chairman JCS, Administrator GSA, Dir. FBI, Dir. Fed. Emergency Management Agency, Chief of Staff Army, Navy, Air Force, Marine Corps, Director DIA, Director NSA, Manager of National Communications System.

Public Law 100-235, Computer Security Act of 1987, January 1988 [CSA87]

Purpose: Provides for a computer standards program within the (renamed) National Institute for Standards and Technology (NIST) to provide for Government-wide computer security, and to provide for the training in security matters of persons who are involved in the management, operation, and use of Federal computer systems. This law has four stated purposes:

1. assigns to NIST the responsibility for developing standards and guidelines for Federal computer systems, including responsibility for developing standards and guidelines drawing on the technical advice and assistance of NSA;
2. provides for the promulgation of such standards and guidelines;
3. requires the establishment of security plans by all operators of Federal computer systems that contain sensitive information; and

4. requires mandatory periodic training for all persons involved in management, use, or operation of Federal computer systems that contain sensitive information.

Users: NIST and NSA personnel as well as all managers or operators of Federal computer systems that contain sensitive information.

DCID 1/16, Security of Foreign Intelligence in Automated Data Processing Systems and Networks, Revised 1988 [SFI88]

Purpose: Governs the COMPUSEC activities of the intelligence community. Describes how sensitive information is to be handled by any AIS system. Covers all intelligence and counterintelligence material such as Sensitive Compartmented Intelligence, “Warning Notice, Intelligence Sources and Methods Involved,” and Special Access Programs for Intelligence. Mandates the use of accredited systems.

Users: Members of the intelligence community, contractors who process intelligence on computers, and other users of DoD computers that process intelligence.

DIAM 50-4, Security of Compartmented Computer Operations, June 1980 [SCCO80]

Purpose: Governs the COMPUSEC activities of those parts of DoD that handle intelligence information. In theory, this is the DIA’s (and, therefore, DoD’s) implementation of DCID 1/16.

Users: DoD members that handle intelligence information, such as DIA.

DoE Order 5639.6A, Classified Automated Information System SecurityProgram, July 1994 [CASP94]

Purpose: Governs the COMPUSEC activities of the Department of Energy (DoE) and DoE Contractors. Primarily focuses on the processing of Restricted Data, but it governs all systems that process DoE data. This Order is implemented by DoE M 5639.6A-1 [CASPM94].

Users: Members of the DoE and its contractors that handle Restricted Data, including some of our national laboratories such as Sandia or Lawrence Livermore.

United States Standards and Guidelines

A single complimentary copy of a guideline or standard may be obtained by calling (410) 766-8729, or by written request to:

Department of Defense
National Security Agency
ATTN: X713/Infosec Awareness Division
9800 Savage Road
Ft. George G. Meade, MD 20755-6000

Additional copies of the standards and guidelines may be purchased through:

Superintendent of Documents
U.S. Government Printing Office
Washington, D.C. 20402
Phone (202) 783-3238

Copies of some of these documents are also available in raw ASCII form on NSA's Dockmaster machine. They are located in the directory **`>site>pubs>guidelines`**.

DOD 5200.28-STD, Department of Defense Trusted Computer System Evaluation Criteria (TCSEC), "The Orange Book," December 1985 [TCSEC85]

Purpose: The TCSEC has been developed to serve a number of intended purposes: (1) to provide a standard for manufacturers as to what securityfeatures to build into their new and planned, commercial products in order to provide widely available systems that satisfy trust requirements for sensitive applications, (2) to provide DoD Components with a metric with which to evaluate the degree of trust that can be placed in computer systems for the secure processing of classified/sensitive information, and (3) to provide a basis for specifying security requirements inacquisition specifications. It is typically used as a guide to vendors developing trusted products for evaluation by the NSA and to NSA evaluators performing the evaluations. It should also be used by vendors that are enhancing the security of their products even if they are not going tobe evaluated.

Users: Anyone planning to build and/or use computers to process sensitive or classified information. Typically vendors, evaluators, and procurement officers.

CSC-STD-002-85, DoD Password Management Guideline, April 1985 [PASS85]

Purpose: This document provides a set of good practices related to the use of password-based user authentication mechanisms in automatic data processing systems employed for processing classified and other sensitive information. It provides a set of rules directed towards preventing password compromise.

Users: Anyone designing a password mechanism for user authentication.

CSC-STD-003-85, Guidance for Applying the DoD TCSEC in SpecificEnvironments , June 1985 [ENV85]

Purpose: This document establishes computer security requirements for DoD by identifying the minimum class of system required for a given risk index. Classes are defined by the TCSEC. Note that the recommendations in this document represent the minimum set adequate to provide an acceptable level of security.

Users: System/network developers; acquisitions personnel writing RFPs; Commercial vendors preparing A, B, and C trust class specifications; system security officers; and program managers.

CSC-STD-004-85, Technical Rationale Behind CSC-STD-003-85: Guidance for Applying the DoD TCSEC in Specific Environments, June 1985 [ENVR85]

Purpose: The purpose of this technical report is to present background discussion and rational for [ENV85]. There are two facets to this requiredguidance: (1) establishment of a metric for categorizing systems according tothe security protection they provide, and (2) identification of the minimum security protection required in different environments.

Users: All DoD components and Departments of the Military whose goal is to provide practical and available security to those systems that will process sensitive and classified information.

NCSC-TG-001, Version 2, A Guide to Understanding Audit in Trusted Systems, June 1988 [AUDIT88]

Purpose: This guideline discusses issues involved in implementing and evaluating an audit mechanism. Its purpose is twofold: (1) provide guidance to developers on how to design and incorporate an effective audit mechanism into their system and (2) provide guidance to system administrators or security officers on how to make effective use ofthe audit capabilities provided by trusted systems.

Users: Vendors developing an audit mechanism as part of a trusted product and end users that are responsible for the security of a running system.

NCSC-TG-002, Trusted Product Evaluations: A Guide for Vendors, June 1990 [TPE90]

Purpose: This document describes procedures for interacting with NSA when participating in TPEP. It provides information needed to submit a computer product for technical security evaluation and outlines the NSA's responsibilities for positive timely acknowledgments. It specifically covers NSA's relationship with vendors through the completion of the security evaluation process and follow-on programs.

Users: Vendors developing or considering the development of a trusted product for evaluation by the NSA.

NCSC-TG-003, A Guide to Understanding Discretionary Access Control inTrusted Systems, September 1987 [DAC87]

Purpose: This guide discusses issues involved in designing, implementing and evaluating discretionary access control (DAC) mechanisms. Its primary purpose is to provide guidance to manufacturers on how to select and build effective DAC mechanisms.

Users: Vendors developing a DAC mechanism as part of a trusted product.

NCSC-TG-004, Glossary of Computer Security Terms, October 1988 [GLOSS88]

Purpose: This document provides a standardized set of terms for common understanding to foster meaningful communications.

Users: All personnel working in the computer security field.

NCSC-TG-005, Trusted Network Interpretation (TNI) of the TCSEC, “The Red Book”, July 1987 [TNI87]

Purpose: As with the TCSEC itself, this Interpretation has been prepared for the following purposes:

1. to provide a standard for manufacturers as to what security features and assurance levels to build into their new and planned commercial network products in order to satisfy trust requirements for sensitive applications.
2. to provide a metric by which to evaluate the degree of trust that can be placed in a given network system for processing sensitive information.
3. to provide a basis for specifying security requirements in acquisition specifications.

Users: Vendors developing a network product for evaluation by the NSA, NSA network evaluators, and procurement officers.

NCSC-TG-006, A Guide to Understanding Configuration Management inTrusted Systems, March 1988 [CM88]

Purpose: The primary purpose of this document is to provide guidance to developers of trusted systems on what configuration management is and how it may be implemented in the development life-cycle of a trusted system. This guideline is also designed to provide guidance todevelopers of all systems on the importance of configuration management and how it may be implemented.

Users: Vendors instituting configuration management procedures on a trusted product being evaluated or RAMPed.

NCSC-TG-007, A Guide to Understanding Design Documentation in Trusted Systems, October 1988 [DDOC88]

Purpose: This guide presents a set of good practices related to design documentation in AISs employed for processing classified and other sensitive information. It helps the vendor and evaluator community understand what deliverables are required for design documentation, as well as the level of detail required of the design documentation at all classes of the TCSEC. In addition, recommendations are made in this technical guideline that are not required by the TCSEC.

Users: Vendors writing design documentation for trusted systems to be evaluated by the NSA.

NCSC-TG-008, A Guide to Understanding Trusted Distribution in TrustedSystems , December 1988 [DISTR88]

Purpose: The purpose of this guideline is to provide guidance to vendors oftrusted systems on what trusted distribution is, why it is important, and how to select and implement an effective distribution system to meet the TCSEC trusted distribution requirement.

Users: Vendors developing an A1 trusted system for evaluation by the NSA, and any others that are interested in the trusted distribution of trusted products.

NCSC-TG-009, Computer Security Subsystem Interpretation of the TCSEC, September 1988 [CSSI88]

Purpose: This Interpretation has been prepared for the following purposes:

1. to establish a standard for manufacturers as to what security features and assurance levels to build into their new and planned computer security subsystem products to provide widely available products that satisfy trust requirements for sensitive applications;
2. to provide a metric to evaluate the degree of trust that can be placed in a subsystem for protecting classified and sensitive information;
3. to lend consistency to evaluations of these products by explicitly stating the implications that are in the TCSEC; and
4. to provide the security requirements for subsystems in acquisition specifications.

Users: Vendors developing a subsystem for evaluation by the NSA, NSA subsystem evaluators, and procurement officers.

NCSC-TG-010, A Guide to Understanding Security Modeling in TrustedSystems , October 1992 [MODEL92]

Purpose: The purpose of this guideline is to provide guidance to vendors and evaluators on the construction, evaluation, and use of security policy models for trusted systems and how to meet the TCSEC and TNI security policy modeling requirements at each TCSEC class. It explains the distinction between formal and informal models and the advantages and disadvantages of various modeling techniques.

Users: Vendors developing, or considering the development of, trusted systems as well as NSA evaluators.

NCSC-TG-011, Trusted Network Interpretation Environments Guideline - - Guidance for Applying the TNI, August 1990 [TNIEG90]

Purpose: This Interpretation describes an environmental assessment process that aids in the identification of minimum security protections needed for different trusted computer network environments. Its primary focus is on the AIS hardware, firmware, and software aspects of security.

Users: Program managers, integrators, certifiers and accreditors of trusted computer network environments.

NCSC-TG-013, Version 1, Rating Maintenance Phase: Program Document, June 1989 [RAMP89]

Purpose: This document describes RAMP for current and prospective vendors of trusted systems. The requirements within this document have been superseded by [RAMP94]. The example process and historical perspective within this document are still relevant to the current RAMP process. However, all actual requirements are contained in the new document.

Users: Vendors and evaluators that are involved in RAMP for an NSA evaluated trusted product or are considering the development of a trusted product for evaluation by the NSA.

Update for NCSC-TG-013, Rating Maintenance Phase: Program Document, Version 2, March 1994 [RAMP94]

Purpose: This document, which is not as yet a formal member of the "Rainbow Series," updates the RAMP requirements contained in [RAMP89]. These new requirements clarify what results are required of a vendor's RAMP process and reduce the amount of requirements on the process itself, thus allowing for more flexibility on the part of the vendor toimplement a RAMP process that meets the requirement of RAMP within the vendor's existing development and maintenance structure.

Users: Vendors and evaluators that are involved in RAMP for an NSA evaluated trusted product or are considering the development of a trusted product for evaluation by the NSA.

NCSC-TG-014, Guidelines for Formal Verification Systems, April 1989 [VERIF89]

Purpose: This document explains the requirements for formal verification systems that are candidates for the NSA's Endorsed Tools List. Use of one of these endorsed tools for formal verification is required for A1 systems.

Users: Developers and NSA evaluators involved in the development or endorsement of such systems.

NCSC-TG-015, A Guide to Understanding Trusted Facility Management, October 1989 [TFM89]

Purpose: This guide presents the issues involved in designing trusted facility management functions to meet the requirements of classes B2 through A1, and discusses how to use these functions effectively. It includes discussions on inherent vulnerabilities of administrative roles, TCSEC requirements and recommendations for each class, separation of operator and administrator roles and possible partitioning of security functions, and impact of other TCSEC requirements on trusted facility management.

Users: Vendors, evaluators, certifiers, accreditors and users of trusted systems being developed, evaluated, certified or operated at class B2 or above.

NCSC-TG-016, Guidelines for Writing Trusted Facility Manuals, October 1992 [TFM92]

Purpose: This document provides a set of good practices related to the documentation of trusted facility management functions of trusted systems. The Trusted Facility Manual (TFM) documents how to configure and install a specific secure system, operate the system ina secure manner, and make effective use of the system privileges and protection mechanisms to control access to administrative functions and database.

Users: Vendors, evaluators, certifiers, accreditors and users of trusted systems.

NCSC-TG-017, A Guide to Understanding Identification and Authenticationin Trusted Systems, September 1991 [I&A91]

Purpose: This document provides guidance to vendors on how to design and incorporate effective identification and authentication (I&A) mechanisms into their systems. It's also written to help vendors and evaluators understand I&A requirements for classes C1 through A1 of the TCSEC. It discusses the purpose of I&A, how I&A works, what are the typical aspects of effective authentication, the importance of securing authentication data, and describes some possible methods of implementation.

Users: Vendors, evaluators, certifiers, accreditors and users of trusted systems.

NCSC-TG-018, A Guide to Understanding Object Reuse in Trusted Systems, July 1992 [OR92]

Purpose: This document describes the TCSEC object reuse requirement and provides guidance for vendors on how to design and incorporate effect object reuse mechanisms into their systems.

Users: Vendors developing, or considering the development of, trusted systems as well as NSA evaluators.

NCSC-TG-019, Trusted Product Evaluation Questionnaire, May 1992 [QUEST92]

Purpose: The purpose of this document is to assist system developers and vendors as a data gathering tool for formalizing the data gathering process for the various phases of TPEP. It consists of 185 questions about various aspects of a secure system. By answering these questions, the vendor should gain a more in-depth understanding of the requirements placed on their own system and how their system meets, or intends to meet, these requirements. The answers to these questions should provide a reasonably concise guide to how the system implements many of the requirements for their particular evaluation class. These answers should be a valuable resource for the developers as well as the NSA's evaluators throughout development and evaluation.

Users: Vendors developing, or considering the development of, trusted systems as well as NSA evaluators.

NCSC-TG-020-A, Trusted Unix® Working Group (TRUSIX) Rationale for Selecting Access Control List Features for the Unix® System, August 1989 [ACL89]

Purpose: This document provides an analysis of key issues involved in extending the discretionary access control (DAC) in the Unix® system. By addressing class B3, this guidance is also helpful in understanding how

Interpretations will be made at B2 and below. The guideline discusses alternative methods for implementing access control lists (ACLs) inthe Unix® system and the relationship of the ACL mechanism to the existing DAC protection mechanism.

Users: Vendors and evaluators involved in the development or evaluation of a trusted Unix® system.

NCSC-TG-021, Trusted Database Management System Interpretation(TDI) of the TCSEC, April 1991 [TDI91]

Purpose: This Interpretation has been prepared for the following purposes:

1. to establish a standard for manufacturers as to what security features and assurance levels to build into their new and planned database management system (DBMS) products in order to satisfy trust requirements for sensitive applications;
2. to provide a metric to evaluate the degree of trust that can be placed in a DBMS for protecting classified and sensitive information;
3. to lend consistency to evaluations of these products by explicitly stating the implications that are in the TCSEC; and
4. to provide the security requirements for DBMSs in acquisition specifications.

Users: Vendors that are considering the development or are developing a trusted DBMS for evaluation by NSA.

NCSC-TG-022, A Guide to Understanding Trusted Recovery in TrustedSystems , December 1991 [RECOV91]

Purpose: This guide presents the issues involved in the design of trustedrecovery mechanisms for trusted systems. It provides guidance to manufacturers on what functions of trusted recovery to incorporate into their systems. It also provides guidance to system evaluators and accreditors on howto evaluate the design and implementation of trusted recovery functions.

Users: Vendors of trusted products and evaluators and accreditors of trusted products or systems.

NCSC-TG-023, A Guide to Understanding Security Testing and Test Documentation in Trusted Systems, July 1993 [STTD93]

Purpose: This guideline provides an in-depth guide to security testing, emphasizing the testing of systems to meet the TCSEC requirements. It gives system developers and vendors suggestions and recommendations on how to develop testing and testing documentation that will be found acceptable by an evaluation team. At C2 and B1, the documentation guidance in this guide is superseded by [VTD94].

Users: Personnel responsible for testing of AIS components.

NCSC-TG-024, A Guide to Procurement of Trusted Systems, Vols. 1-4, February 1994 [PROC94]

Purpose: This four-volume set of procurement guidelines was developed to clarify how to use the TCSEC in the acquisition of trusted systems. It provides procurement initiators with an introduction to computer security requirements, with language for Request for Proposal (RFP) specifications and statements of work, and with a computer security contract data requirements list and a data item description tutorial.

Users: Personnel responsible for procurement of trusted AIS components.

NCSC-TG-025, Version 2, A Guide to Understanding Data Remanence in Automated Information Systems, September 1991 [REMAN91]

Purpose: This second version of the guideline replaces the previous version *DoD Magnetic Remanence Security Guideline*, CSC-STD-005-85, dated 15 November 1985. It provides information to personnel responsible for the secure handling of sensitive AIS memory and secondary storage media. It also provides information related to the clearing, purging, declassification, destruction, and release of most AIS storage media.

Users: Personnel responsible for the secure handling of sensitive AIS memory and secondary storage media and for vendors of AIS components.

NCSC-TG-026, A Guide to Writing the Security Features User's Guide for Trusted Systems, September 1991 [SFUG91]

Purpose: This guideline explains the motivation and meaning of the TCSEC requirement for a Security Features User's Guide (SFUG). It identifies and discusses the considerations that influence the development and evaluation of an SFUG, such as its audience, content, and organization. It discusses various approaches to writing an SFUG that have been accepted by trusted product evaluators in the past.

Users: Any potential author or evaluator of an SFUG, whether a product vendor, system integrator, evaluator, certifier, accreditor or user.

NCSC-TG-027, A Guide to Understanding Information System SecurityOfficer Responsibilities for Automated Information Systems, May 1992 [ISSO92]]

Purpose: This guideline identifies system security responsibilities forInformation Systems Security Officers (ISSOs). It applies to computersecurity aspects of AISs within the DoD and its contractor facilities thatprocess classified and sensitive unclassified information. It also discusses the roles and responsibilities of other individuals who are responsible for security and their relationship to the ISSO.

Users: ISSOs who are responsible for implementing and maintaining security in a system, as well as vendors developing those systems and evaluators assessing those systems.

NCSC-TG-028, Assessing Controlled Access Protection, May 1992 [ACAP92]

Purpose: This guideline provides a methodology for performing a technical analysis to support the certification of controlled access protectionin AISs submitted for accreditation. It provides an interim approach for achieving controlled access protection until a suitable NSA-evaluated product is available. It also clarifies the intent, security functionality, and level of protection that controlled access protection provides.

Users: Technical analysts tasked by DoD components to determine whether a system meets the TCSEC controlled access protection requirements.

NCSC-TG-029, Introduction to Certification and Accreditation, January 1994 [C&A94]

Purpose: This document initiates a sub-series on certification andaccreditation (C&A) guidance. It provides an introduction to C&A, and should be viewed as guidance in meeting requirements for C&A of AISs. The details of the actual C&A process are not included in this document, but will be provided in a follow-on document(s)

Users: System accreditors, certifiers, integrators, and engineers; program managers, developers, security officers, evaluators, and users.

NCSC-TG-030, A Guide to Understanding Covert Channel Analysis in Trusted Systems, November 1993 [COVERT93]

Purpose: This guideline presents the relative merits of covert channel identification methods and of covert channel information sources, recommends sound bandwidth determination and handling policies and methods based on the TCSEC requirements, and defines the types of evidence that should be provided for handling assurance.

Users: Vendors developing, or considering the development of, trusted systems as well as NSA evaluators.

Form and Content of Vendor Design Documentation, May 1994 [VDD94]

Purpose: This document, which is not as yet a formal member of the “Rainbow Series,” specifies the development of three additional summary documents for C2 and B1 evaluations. The required content and recommended organization of the three additional documents are stated and illustrated with examples.

Users: Vendors and evaluators participating in a C2 or B1 evaluation.

Form and Content of Vendor Test Documentation, May 1994 [VTD94]

Purpose: This document, which is not as yet a formal member of the “Rainbow Series,” specifies the development of an additional test document for C2 and B1 evaluations. The required content and recommended organization of this document is defined, and guidance is supplied concerning the documentation of test plans, procedures, and results.

Users: Vendors and evaluators participating in a C2 or B1 evaluation.

The Interpreted TCSEC Requirements, published quarterly [INTERP94]

Purpose: This clarification of TCSEC requirements contains Interpretations resulting from specific questions raised during evaluations, and attempts to build a body of "case law" by documenting system-specific clarifications rather than providing general, all-encompassing Interpretations. It is maintained in PostScript format on Dockmaster as **>udd>CPE>public>iwg>Interpreted.TCSEC.YY-MM-DD.ps**, where "**YY-MM-DD**" represents the date of publication.

Users: Anyone making use of the TCSEC requirements. Typically vendors, evaluators, and procurement officers.

Other Pertinent Documents

A single copy or a one year subscription to the quarterly InformationSystems Security Products and Services Catalog may be purchased through:

Superintendent of Documents
U.S. Government Printing Office
Washington, D.C. 20402
Phone (202) 783-3238

The Technical Assessment Report (TAR) on a specific verification tool done as part of the verification assessment study can be obtained by contactingthe Office of Information System Security Research and Technology:

Department of Defense
ATTN: R206
9800 Savage Road
Fort Meade, MD 20755-6000

GPO 908-027-00000-1, Information Systems Security Products and ServicesCatalog , published quarterly [ISSP94]

Purpose: Serves as a source document and working aid for those who have established a need for information system security products or services. Provides general information and points of contact for each product or service identified. The document is published on a quarterly basiswith updates to the following lists of products or services:

- Endorsed Cryptographic Products List

  The NSA has established an inventory of cryptographic and related items which carry an NSA endorsement. This endorsement means that the communications security subsystem has been certified as having met the appropriate minimum Agency security requirements and is therefore endorsed for use to secure the applicable level of government information.

- Potential Cryptographic Products List

  Contains the names of companies and their respective products that have been accepted into the Commercial COMSEC Endorsement Program through the signing of a Memorandum of Understanding.

When a product achieves NSA security endorsement, it is placed on the Endorsed Cryptographic Products List.

- Endorsed Data Encryption Standard Products List

  The Data Encryption Standard has been identified as an appropriate cryptographic technique for protecting sensitive, but unclassified information. This chapter contains a description of the Government endorsed voice and data encryption devices, a list of data required for ordering keying material, and points of contact.

- Protected Services List

  Telecommunications systems, approved by NSA for the transmission of certain types of sensitive U.S. Government information, that are available from common carrier communications companies.

- Endorsed Tools List

  This list identifies the formal specification and verificationtools that are endorsed by the NSA for use in designing candidate A1 systems.

- Degausser Products List

  Lists the model identification of equipment units that were evaluated against and found to satisfy the requirements for erasure of magnetic media that hold classified data. This list is no longer maintained by NSA.

- Evaluated Products List

  Lists products that have been evaluated against the TCSEC by the NSA and have been assigned a rating. The rating reflects the highest class for which the product satisfies all the TCSEC requirements for that class. Products are separated into general purpose operating systems, add-on packages and subsystems.

- Preferred Products List

  List of commercially developed and produced TEMPEST telecommunications equipment accredited as meeting the TEMPEST requirements. Products on this list were designed, developed and manufactured by companies which were members of the NSA Industrial TEMPEST Program. Numerous products are still valid, however, this program has been replaced by the Endorsed TEMPEST Products Program.

- Endorsed and Potential TEMPEST Products List

  Replaces the Preferred Products List. The old program was based on membership in the program, while the new program emphasizes individual product or service endorsement.

Users: U. S. Government agencies and departments, government contractors, and vendors building, procuring or operating secure products.

NCSC-C3-Cr01-86, Verification Assessment Study Final Report, Vols. I-V., March 1986 [Kemme86a] (restricted distribution)

Purpose: Contains a summary of verification topics and reports conclusions based on the study of four verification systems. Provides a limited view of the complete topic of formal verification. This first volume outlinesthe approach taken, summarizes the results of the study and suggests further research. The remaining four volumes each were dedicated to a separate verification system. These were: Gypsy, Affirm, FDM and Enhanced HDM.

Users: Anyone interested in the use of the particular verification environment studied or interested in developing a formal verification system.

C Technical Report 79-91, Integrity in Automated Information Systems, September 1991 [Mayfield91]

Purpose: Provides a framework for examining integrity in computing and an analytical survey of techniques that have potential to promote and preserve computer system and data integrity. It is intended as a general foundation for further investigations into integrity and as a focus for debate on those aspects of integrity related to computer and automated information systems.

Users: System designers, criteria developers, and individuals trying to gain a better understanding of the issues of data and systems integrity.

Relevant Trusted Product Evaluation Questionnaire Questions

None.

Required Readings

Gangem90 Gangemi, G.T., Chapter 2 of the book *Secure Systems Long Range Strategic Plan*, to be published by Wang Laboratories, Inc., 1990.

This chapter of Gangemi's book provides an excellent description of the history of INFOSEC, COMSEC, and COMPUSEC from the early days of computer security to the present day.

Supplemental Readings

ACAP92 National Computer Security Center, *Assessing Controlled Access Protection*, NCSC-TG-028, Version 1, 25 May 1992.

ACL89 National Computer Security Center, *Trusted Unix Working Group (TRUSIX) Rationale for Selecting Access Control List Features for the Unix® System*, NCSC-TG-020-A, Version 1, 18 August 1989

AUDIT88 National Computer Security Center, *A Guide to Understanding Audit in Trusted Systems*, NCSC-TG-001, Version 2, 1 June 1988.

C&A94 National Computer Security Center, *Introduction to Certification and Accreditation*, NCSC-TG-029, Version 1, January 1994.

CM88 National Computer Security Center, *A Guide to Understanding Configuration Management in Trusted Systems*, NCSC-TG-006, Version 1, 28 March 1988.

COVERT93 National Computer Security Center, *A Guide to Understanding Covert Channel Analysis of Trusted Systems*, NCSC-TG-030, Version 1, November 1993.

CSSI88 National Computer Security Center, *Computer Security Subsystem Interpretation of the TCSEC,* NCSC-TG-009, Version 1, 16 September 1988.

DAC87 National Computer Security Center, *A Guide to Understanding Discretionary Access Control in Trusted Systems*, NCSC-TG-003, Version 1, 30 September 1987.

DDOC88 National Computer Security Center, *A Guide to Understanding Design Documentation in Trusted Systems*, NCSC-TG-007, Version 1, 2 October 1988.

DISTR88 National Computer Security Center, *A Guide to Understanding Trusted Distribution in Trusted Systems,* NCSC-TG-008, Version 1, 15 December 1988.

ENV85 DoD Computer Security Center, *Guidance for Applying the DoD TCSEC in Specific Environments*, CSC-STD-003-85, June 1985.

ENVR85 DoD Computer Security Center, *Technical Rationale Behind CSC-STD-003-85: Guidance for Applying the DoD TCSEC in Specific Environments*, CSC-STD-004-85, 25 June 1985.

GLOSS88 National Computer Security Center, *Glossary of Computer Security Terms*, NCSC-TG-004, Version 1, 21 October 1988.

I&A91 National Computer Security Center, *A Guide to Understanding Identification and Authentication in Trusted Systems,* NCSC-TG-017, Version 1, September 1991.

INTERP94 National Computer Security Center, *The Interpreted TCSEC Requirements*, (quarterly).

ISSO92 National Computer Security Center, *A Guide to Understanding Information System Security Officer Responsibilities for Automated Information Systems*, NCSC-TG-027, Version 1, May 1992.

MODEL92 National Computer Security Center, *A Guide to Understanding Security Modeling in Trusted Systems*, NCSC-TG-010, Version 1, October 1992.

OR92 National Computer Security Center, *A Guide to Understanding Object Reuse in Trusted Systems,* NCSC-TG-018, Version 1, July 1992.

PASS85 National Computer Security Center, *DoD Password Management Guideline*, CSC-STD-002-85, April 1985.

PROC94 National Security Agency, *A Guide to Procurement of Trusted Systems*, NCSC-T9-024, Version 1, Vols. 1-4, February 1994.

QUEST92 National Computer Security Center, *Trusted Product Evaluation Questionnaire*, NCSC-TG-019, Version 2, 2 May 1992.

RAMP89 National Computer Security Center, *Rating Maintenance Phase: Program Document*, NCSC-TG-013, Version 1, 23 June 1989.

RAMP94 National Computer Security Center, *Rating Maintenance Phase: Program Document*, Draft, Version 2, 1 March 1994.

RECOV91 National Computer Security Center, *A Guide to Understanding Trusted Recovery in Trusted Systems*, NCSC-TG-022, Version 1, 30 December 1991.

REMAN91 National Computer Security Center, *A Guide to Understanding Data Remanence in Automated Information Systems,* NCSC-TG-025, Version 2, September 1991.

SFUG91 National Computer Security Center, *A Guide to Writing the Security Features User's Guide for Trusted Systems*, NCSC-TG-026, Version 1, September 1991.

STTD93 National Computer Security Center, *A Guide to Understanding Security Testing and Test Documentation in Trusted Systems*, NCSC-TG-023, Version 1, July 1993.

TCSEC85 National Computer Security Center, *Department of Defense Trusted Computer Security Evaluation Criteria,* DoD 5200.28-STD, December 1985.

TDI91 National Computer Security Center, *Trusted Database Management System Interpretation of the TCSEC*, NCSC-TG-021, Version 1, April 1991.

TFM89 National Computer Security Center, *A Guide to Understanding Trusted Facility Management*, NCSC-TG-015, Version 1, 18 October 1989.

TFM92 National Computer Security Center, *Guidelines for Writing Trusted Facility Manuals*, NCSC-TG-016, Version 1, October 1992.

TNI87 National Computer Security Center, *Trusted Network Interpretation of the TCSEC*, NCSC-TG-005, Version 1, July 1987.

TNIEG90 National Computer Security Center, *Trusted Network Interpretation Environment Guideline -- Guidance for Applying the TNI*, NCSC-TG-011, Version 1, 1 August 1990.

TPE90 National Computer Security Center, *Trusted Product Evaluations: A Guide for Vendors*, NCSC-TG-002, Version 1, 22 June 1990.

VDD94 National Computer Security Center, *Form and Content of Vendor Design Documentation*, Draft, May 1994.

VERIF89 National Computer Security Center, *Guidelines for Formal Verification Systems*, NCSC-TG-014, Version 1, 1 April 1989.

VTD94 National Computer Security Center, *Form and Content of Vendor Test Documentation*, Draft, May 1994.

Other Readings

ADPSM79 Department of Defense, *ADP Security Manual -- Techniques and Procedures for Implementing, Deactivating, Testing, and Evaluating Secure Resource-Sharing ADP Systems*, DoD 5200.28-M, June 1979.

AIS88 Department of Defense, *Security Requirements for Automated Information Systems*, DoD 5200.28, March 1988.

CASP94 Department of Energy, *Classified Automated Information System Security Program*, DoE Order 5639.6A, July 1994.

CASPM94 Department of Energy, *Manual of Security Requirements for the Classified Automated Information System Security Program*, DoE M 5639.6A-1, July 1994.

CSA87 U.S. Congress, *Computer Security Act of 1987*, HR145, Public Law 100-235, 8 January 1988.

CSEC81 Department of Defense, *Computer Security Evaluation Center*, DoD 5215.1, 1981.

ISM91 Department of Defense, *Industrial Security Manual for Safeguarding Classified Information*, DoD 5220.22-M, January 1991.

ISMM87 Department of Defense, *Marking Supplement to Industrial Security Manual for Safeguarding Classified Information*, DoD 5220.22-S-2, September 1987.

ISPR87 Department of Defense, *Information Security Program Regulation*, DoD 5200.1-R, April 1987.

ISR84 Department of Defense, *Industrial Security Regulation*, DoD 5220.22-R, February 1984.

ISSP94 National Security Agency, *Information Systems Security Products and Services Catalog*, GPO 908-027-00000-1, (quarterly).

Kemme86a Kemmerer, R., *Verification Assessment Study Final Report*, NCSC-C3-Cr01-86, Vols. I-V, March 1986.

Mayfield91 National Computer Security Center (Mayfield, W.T., et. al.), *Integrity in Automated Information Systems*, C Technical Report 79-91, September 1991.

MFIR94 Office of Management and Budget, *Management of Federal Information Resources*, OMB Circular A-130, July 1994.

NSI82 President of the United States, *National Security Information*, E.O. 12356, 6 April 1982.

NSTIS90 President of the United States, *National Policy for the Security of National Security Telecommunications and Information Systems*, NSD-42, July 1990.

SCCO80 Defense Intelligence Agency, *Security of Compartmented Computer Operations (U) (CONFIDENTIAL)*, DIAM 50-4, Washington, DC, June 1980.

SFI88 Director of Central Intelligence, *Security of Foreign Intelligence in Automated Data Processing Systems and Networks (U) (SECRET)*, DCID 1/16, Washington, DC, revised 1988.